UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,969	06/27/2001	Steven A. Bade	AUS920010358US1	3816

35525 7590 11/18/2004

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
HO, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,969	BADE, STEVEN A.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-3, 6, 8, 9-11, 14, 16-19, 22, 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Weeks et al. "CCI-Based Web Security: A Design Using PGP".

In reference to claim 1:

Weeks et al. discloses a method in a data processing system, said method comprising the steps of:

- Receiving a request for a secure Web page, said secure web page including data, where the request for a secure webpage is website that has been encrypted with PGP. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")
- Determining whether said data has been pre-encrypted, where it is known if the website has been encrypted with PGP if it has the extension .pgp. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")

- Bypassing an encryption step and transmitting said data in response to a determination that said data has been pre-encrypted, where the pgp file is served or transmitted to the client, if it has already been encrypted with PGP and has a .pgp extension. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")

In reference to claim 2:

Weeks et al. (Page 7, "The PGP-CCI Protocol") discloses the method according to claim 1, further comprising the step of in response to a determination that said data has not been pre-encrypted, encrypting said data and transmitting said encrypted data, where the website, if it has not yet been encrypted with PGP, is sent to be encrypted or signed with a PGP key.

In reference to claim 3:

Weeks et al. (Page 6, "Storing PGP-Enhanced Documents as a Web Server") discloses the method according to claim 2, further comprising the step in response to a determination that said data has not been pre-encrypted, storing said encrypted data, where if the original html file or document at the URL has not yet been pre-encrypted, it is encrypted with a PGP key, and it's extension is then changed to .pgp to be stored as a new file type.

In reference to claim 6:

Weeks et al. discloses the method according to claim 1, further comprising the steps of:

- Receiving said request for said secure web page. Said secure web page including static information has been pre-encrypted, where the request for a secure webpage is a request

for a website that has been PGP encrypted. (Page 6, "Viewing PGP-Enhanced Documents")

- Bypassing an encryption step and transmitting said static information in response to a determination that said static information has been pre-encrypted, where if the html file has already been pre-encrypted, it has the extension .pgp and is not further encrypted, but sent as a .pgp file as evidenced by the necessity of a MIME type. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")
- Encrypting said dynamically-changing information, where the dynamically changing information is information transmitted in a form which is made part of the URL request in the POST operation of HTML, which is then encrypted using PGP. (Page 13, "Client Operation")
- Transmitting said encrypted, dynamically-changing information, where the encrypted PGP information is then transmitted. (Page 13, "Client Operation")

In reference to claim 8:

Weeks et al. discloses the method according to claim 1, further comprising the step of maintaining said web page by a secure web site, where the PGP-enhanced document system is a method of maintaining a webpage by a secure website, secure through PGP.

Claims 9, 17 are rejected for the same reasons as claim 1.

Claims 10, 18 are rejected for the same reasons as claim 2.

Claims 11, 19 are rejected for the same reasons as claim 3.

Claims 14, 22 are rejected for the same reasons as claim 6.

Claims 16, 24 are rejected for the same reasons as claim 8.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4,5,7, 12, 13, 15, 20, 21, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weeks et al. "CCI-Based Web Security: A Design Using PGP".

In reference to claim 4:

Weeks et al. fails to explicitly disclose a method according to claim 3, further comprising the step of storing said encrypted data in a cache.

Weeks et al. does, however disclose that the encrypted data is stored. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")

The Examiner takes official notice that storing encrypted data in a cache was well known in the art at the time of invention. In fact, storing encrypted data in a cache is usually expected. A cache is a region of memory, usually smaller than a regular or main block of memory or space, from which data will be frequently accessed. Cache is a memory concept, present in RAM, Hard Disk space, and processor memory, as a secondary storage used to quickly access data that has recently been retrieved. By the concept of temporal locality, a piece of information on a

computer recently accessed, is likely to be accessed again in the near future. Caching the is action of storing into the cache, information that has been accessed recently.

It would have been obvious to one of ordinary skill in the art at the time of invention to store the encrypted data in a cache in order to provide the advantage of quickly supplying the data without the full latency of a regular access, if the user decides to use the data again.

In reference to claim 5:

Weeks et al. discloses all of method according to claim 1, further comprising the steps of:

- Receiving a request for an image included within said web page, where the image data is a graphic on a website (page 7, paragraph 2)
- Checking memory to determine whether a pre-encrypted version of said image is already stored in said memory, where the pre-encrypted version is the .pgp HTML file. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")
- In response to a determination that said pre-encrypted version is stored in said memory, bypassing an encryption step and transmitting said pre-encrypted version, where the encryption step is bypassed in that the .pgp is sent to the user, without need for a further encrypted on top of the already encrypted .pgp file. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")
- In response to a determination that said pre-encrypted version is not stored in said memory, encrypting said image and transmitting said encrypted image, where before a file was originally stored as a .pgp file, it was recognized as not having been encrypted,

and thus signed in order to form the .pgp file. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")

Weeks et al. however fails to disclose the case, where the storage used is cache.

It would have been obvious to one of ordinary skill in the art at the time of invention to cache the encrypted .pgp files in order to quickly supply the files again to the user should they be needed in the near future.

In reference to claim 7:

Weeks et al. discloses the method according to claim 1, wherein said data processing system further includes a server computer system coupled to a client computer system utilizing a network, said method further comprising the steps of:

- Receiving a request for said web page by said server (Page 6, "Viewing PGP Enhanced Documents")
- Determining whether a pre-encrypted version of said data has been stored in said memory in response to said receipt of said request. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")
- In response to a determination that said pre-encrypted version of said data has not been stored in said memory, encrypting said data and transmitting said encrypted data. (Page 7, "The PGP-CCI Protocol", Item 2)

- In response to a determination that said pre-encrypted version of said data has been stored in said memory, transmitting said pre-encrypted version of said data. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")

Weeks et al. fails to explicitly disclose:

- Establishing a secure sockets layer (SSL) session between client and said server in response to said client transmitting said request
- Associating a cache with said SSL session
- Storing the data in memory where the memory is a cache.

The Examiner takes official notice that the use of SSL, or the Secure Sockets Layer was well known in the art at the time of invention. Secure Sockets Layer is a well known protocol widely used in Internet transactions because of its balance with respect to speed and security. E-commerce websites and banks that use SSL all employ the https:// as opposed to http://
To this effect, the use of SSL is ubiquitous.
It would have been obvious to one of ordinary skill in the art at the time of invention to use SSL in the web transactions between the client and the server and store accessed data in a cache in order to encrypt the data transmitted in order to encrypt the data in such a way that was widely used and supported by the dominant web browsers, and leave in a location for faster access times in the near future.

Claims 12, 20 are rejected for the same reasons as claim 4.

Claims 13, 21 are rejected for the same reasons as claim 5.

Claims 15, 23 are rejected for the same reasons as claim 7.

Conclusion

5. The following prior art not relied upon is made of record.

McDonnal et al. US patent 5,796,825 discloses the use automatic decryption and reencryption of files that are accessed from a file system in which files are stored in their encrypted versions. McDonnal also discloses the bypassing of unnecessary re-encryption for files that have already been encrypted.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (571)272-3838. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

November 11th, 2004

TMH